(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 422 230 A1**

(12) **EUROPEAN PATENT APPLICATION published in accordance with Art. 158(3) EPC**

(21) Application number: **90902392.1**

(22) Date of filing: **24.01.90**

(86) International application number: **PCT/JP90/00078**

(87) International publication number: **WO 90/09009 (09.08.90 90/19)**

(51) Int. Cl.[5]: **G06K 19/073**, G06K 17/00, G09C 1/00

(30) Priority: **24.01.89 JP 15329/89**
24.01.89 JP 15336/89

(43) Date of publication of application: **17.04.91 Bulletin 91/16**

(84) Designated Contracting States: **DE FR GB**

(71) Applicant: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD**
1006, Ohaza Kadoma, Kadoma-shi
Osaka 571(JP)

(72) Inventor: **TAKAGI, Nobuya**
11-5, Suehiro-cho Neyagawa-shi
Osaka 572(JP)
Inventor: **ITO, Mamoru**
10-30-207, Koshiensanban-cho
Nishinomiya-shi
Hyogo 663(JP)
Inventor: **TSUJI, Toshio**
6-15-6, Amamihigashi Matsubara-shi
Osaka 580(JP)

(74) Representative: **Dr. Elisabeth Jung Dr. Jürgen Schirdewahn Dipl.-Ing. Claus Gernhardt**
P.O. Box 40 14 68 Clemensstrasse 30
W-8000 München 40(DE)

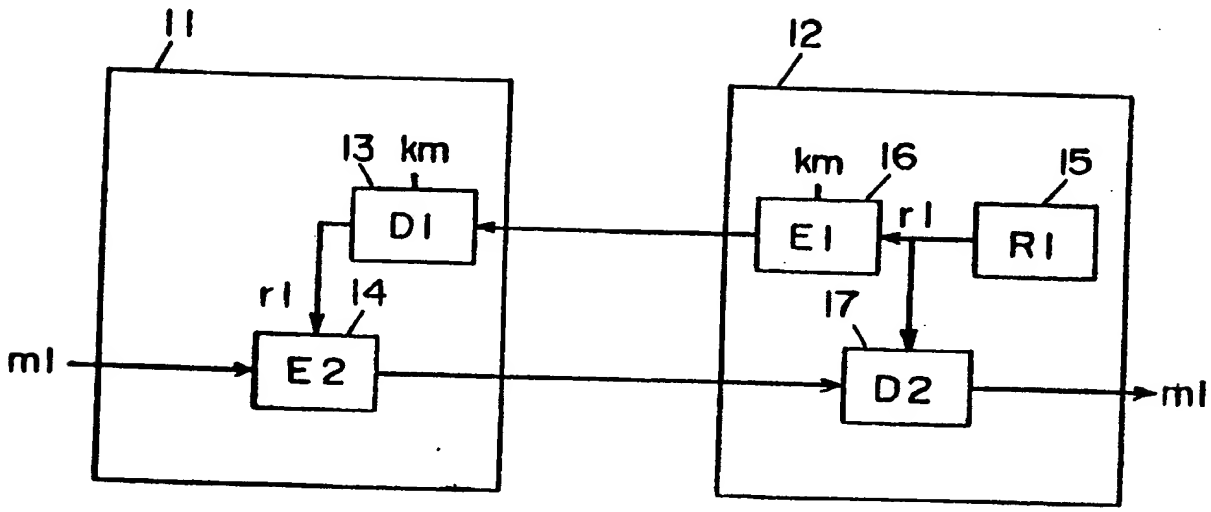
(54) **DATA CARRIER AND DATA COMMUNICATION APPARATUS USING THE SAME.**

(57) A data carrier such as an IC card and a data communication apparatus using the same, wherein contrivance is made to prevent eavesdropping of data from the communication wire. To achieve this according to the invention, a session key (r1) generated from a random number forming means (15) is ciphered by cipher means (16) using a master key (km) and is sent to an external unit. Further, a cryptogram input from an external unit is decoded by decoding means (17) using a session key (r1) generated from the random number forming means (15).

EP 0 422 230 A1

BNSDOCID: <EP___0422230A1_I_>

FIG. 2



BNSDOCID: <EP___0422230A1_I_>

DATA CARRIER AND DATA COMMUNICATION APPARATUS USING IT

TECHNICAL FIELD

The present invention relates to a data carrier such as an IC card which is usable for cipher communication, and a data communication apparatus using it.

BACK GROUND ART

In order to perform cipher communication in a secret key cipher system, both parties which make communication are required to hold in common a key in advance. Hitherto, sharing of the key has been performed by a system as shown in FIG.11 for example. Referring to FIG.11, numeral 41 designates a coder which is used by a sending party of a message (hereinafter is simply referred to as a sending party), and 42 designates a decoder which is used by a receiving party of the message (hereinafter is simply referred to as a receiving party), and the coder 41 comprises a random number generating means 49, a first enciphering means 44 and a second enciphering means 45, and the decoder 42 comprises a first decoding means 46 and a second decoding means 47.

Operation of the conventional common ownership system of the key composed like this is described hereafter. Since the key for enciphering a plain text of a message (hereinafter is simply referred to as a plain text) m is required to be changed frequently from the aspect of safety, a random number which is generated by the random number generating means 43 is used. Hereinafter, this is described as a session key. The sending party sends an output r1 (it is called a session key as another name) of the random number generating means 43 which is held in the coder 41 to the receiving party in order to hold in common with the receiving party; but if r1 is sent as the sate of raw data it is liable to be tapped on the communication line between the coder 41 and the decoder 42, and hence r1 is enciphered by the enciphering means 44 and is sent. The key which is used to encipher r1 is called as a master key km, and it is the key which is held in common by the sending party and receiving party in advance. The master key is used only when the session key is sent by enciphering, and is generally fixed during a long time period. The decoder 42 of the receiving party decodes the enciphered random number by the master key km and restores r1 by using the first decoding means 46. Thereby, since the sending party and receiving party have held in common the session key r1, thereafter, cipher communication of the plain text m can be accomplished by the session key r1 by using the second enciphering means 45 and the second decoding means 47. In the event that the session key is changed, a new random number r2 (not shown) is generated by the random number generating means 43; and in the same manner as described above, r2 is held in common by the cipher communication by means of the master key km and is made to the session key.

Now, the case of cipher communication between two communication parties A and B is assumed. The communication party A and the communication party B encipher the session key r1 by using the master key km and send. When another communication party C holds the master key km, all cipher text which is exchanged between the communication parties A and B can be deciphered since the communication party C can decipher the session key r1. Therefore, it is required that the master key km is known by only the communication party A and the communication party B, and in the event that, for example, the communication party A carries out cipher communication with the communication party C, a master key which is other than km is used. Namely, the communication party A must hold the master keys which are identical with the number of the parties which carry out the cipher communication.

In such conventional system, there is no problem in the event of a small number of parties are to be communicated; but in a network having unspecified many subscribers, communication parties to be communicated become large number, and management of the key becomes a big problem. As a means for solving it, the method in which a center for performing management of the key is provided, and prior to prosecution of the cipher communication, the center delivers (or transmit) the common session key to both the parties, is generalized, but there is a defect that the center must intervene in every common holding operation of the key. On the other hand, as other solution, there is a method using the public key cipher system which is superior in management of the key, but the public key cipher system entails a much longer processing time in comparison with the secret key cipher system. As mentioned above, in the conventional cipher communication method, a big problem has existed with respect to the management of the key.

In view of such a problem, the present invention is directed to provide a data carrier which is safely, easily and speedy realizable common ownership of the key, on the basis of the futures in which an internal

BNSDOCID: <EP___0422230A1_I_>

data is physically safety and calculation ability exist, and a data communication apparatus using it.

DISCLOSURE OF INVENTION

And in order to achieve the object, the data carrier of the present invention has a configuration comprising means for holding a first data which is impossible to be changed to data which is designated from outside, first enciphering means for enciphering the first data by a secret key, first decoding means for decoding a cipher text inputted from outside by said first data, second decoding means for decoding enciphered second data inputted from outside by the second secret key, and a second enciphering means for enciphering a plain text which is inputted from the outside or stored inside by the output of the above-mentioned second decoding means.

The feature of a configuration of the present invention is the point that the first secret key and the second secret key are stored in a memory in the IC card which is physically safe, and the point that a first data which is automatically generated by own IC card as a decoding key is used, and the key generated on the basis of a second data which is sent from the party is used for an enciphering key. Reason that the above-mentioned object is realized by this configuration can be elucidated as follows.

First, since the first secret key and the second secret key are stored in the memory in the IC card which is physically safe, these secret keys can not be read out even by the owner of the IC card. Therefore, without using the IC card which stores these secret keys, the first data and second data can not be restored from the output of the first enciphering means and the enciphered second data which are inputted from the outside. Consequently, the cipher text which is inputted from the outside and the cipher text which is output from the second enciphering means can not be deciphered.

If the second secret key is common to the whole IC cards, an evil-minded person can rebuild the second data in his own IC card by tapping the enciphered second data and inputting it into own IC card. However, the function that the IC card can performs by using the second data is only to encipher, and it has no decoding function. On the other hand, the key for decoding in this IC card is a first data which is automatically generated by own IC card. Namely, the evil-minded third person can not make setting of the decoding key and decoding using the key simultaneously.

From the above-mentioned matter, by the configuration of the IC card of the present invention, the IC card which has generated the first data, namely only the IC card of the receiving party can decode the cipher text, and the cipher communication is made safety. Furthermore, common ownership of the key is easily realized, by using the IC card of the present invention, since both the list of the secret key and the center are not required. Moreover, since it can be composed of only the secret key cipher, high speed processing is made possible.

BRIEF DESCRIPTION OF DRAWINGS

FIG.1 is a figure of a system configuration of a system using an IC card of the present invention, FIG.2 is a block diagram showing the IC card having a key common ownership function in accordance with an embodiment of the present invention, FIG.3 and FIG.10 are block diagrams of the IC cards which configurate a key common ownership system which is not safe, FIG.4, FIG.5, FIG.6 and FIG.9 are block diagrams showing the IC cards having the key common ownership function in accordance with other embodiment of the present invention, FIG.7 is a block diagram showing random number generating means in accordance with an embodiment of the present invention, FIG.11 is the figure of the system configuration showing the conventional key common ownership method.

BEST MODE FOR CARRYING OUT THE INVENTION

FIG.1 is a block diagram showing an example of a data communication apparatus using an IC card which is used as an example of a data carrier of the present invention. Referring to FIG.1, numeral 1 designates a first terminal, numeral 2 designates a second terminal, numeral 3 designates a first IC card having a cipher apparatus 4 in the same body, numeral 5 designates a second IC card having a decoding apparatus 6 in the same body. Moreover, the first terminal 1 comprises an input apparatus 7 and a transmission apparatus 8, and the second terminal 2 comprises an output apparatus 9 and a reception apparatus 10.

BNSDOCID: <EP___0422230A1_I_>

A process for carrying out cipher communication by this system is shown hereafter. First, in starting the cipher communication, a sending party inserts the first IC card 3 in the first terminal 1, and a receiving party inserts the second IC card 5 in the second terminal 2. After then, the sending party inputs a plain text m by using the input apparatus 7. The plain text m is inputted into the first IC card 3, and is converted into a cipher text c by the enciphering apparatus 4 and is output. The first terminal 1 outputs the cipher text c to the second terminal 2 by using the transmission apparatus 8. On the other hand, the receiving party receives the above-mentioned cipher text c by using the reception apparatus 10. The cipher text c is inputted to the second IC card 5, and is decoded to the plain text m by the decoding apparatus 6 and is output. The second terminal 2 outputs the restored plain text m by using the output apparatus 9. A system for carrying out the cipher communication by using the IC card for a cipher apparatus and a decoder in this manner is considered. In carrying out an actual cipher communication, common ownership of the session key is required, as mentioned above. As to this, elucidation is made with reference to the detailed figures of the IC card shown after FIG.2. With respect to FIG.2 and thereafter, the first terminal 1 and the second terminal 2 are omitted in the drawings.

FIG.2 is a block diagram of the IC card in accordance with an embodiment of the present invention. Referring to FIG.2, numeral 11 designates the first IC card, and numeral 12 designates the second IC card. The first IC card 11 comprises first decoding means 13 and second enciphering means 14. Then, the second IC card 12 comprises random number generating means 15, first enciphering means 16 which is paired with the first decoding means 13, the second decoding means 17 which is paired with the second enciphering means 14.

Hereafter, the present embodiment is elucidated in compliance with FIG.2. Since the second IC card 12 holds the key in common, the random number r1 which is output by the random number generating means 15 is enciphered by a master key km by using the first enciphering means 16 and is sent to the first IC card 11. By using the first decoding means 13, the first IC card 11 decodes the enciphered random number by the master key km and restore r1. Thereby, using this as the session key, the cipher communication of the plain text m1 can be carried out by the second enciphering means 14 and the second decoding means 17, since the first IC card 11 and the second IC card 12 hold the random number r1 in common. Therein, master key km is a common value to whole IC cards.

The reason that the key common ownership method shown in FIG.2 is safe is elucidated hereafter. First, since the master key km is stored in the memory in the IC card which is physically safe, the master key km can not be read out even by the owner of the IC card. Therefore, even if the output of the first enciphering means 16 is tapped on the communication line, the random number r1 can not be decoded from the output of the first enciphering means 16 without using the IC card in which the master key km is stored. Consequently, the cipher text output from the second enciphering means 14 can not be deciphered.

Subsequently, the case in which there is three communication parties A, B, C which belong to the system are present, and the C intends to decipher the cipher text which is exchanged between the A and B is considered. Since the C is the communication party which belongs to the system, the C has the first IC card 11 or the second IC card 12. First, the assumption is made that the C has the first IC card 11. If the C taps the output of the first enciphering means 16 which is exchanged between the A and the B, and input it into the own IC card, restoration of the random number r1 in own IC card is possible by the first decoding means 13 and the master key km. However, the function that the IC card can perform by using the random number r1 is only for enciphering by the second enciphering means 14, and there is no decoding function. On the other hand, even if the C has the second IC card 12 having the second decoding means 17, the key in decoding of the IC card is the random number which is automatically generated by the IC card. Namely, the C can not make simultaneously arbitrary setting of the decoding key and decoding process using the key by using own IC card.

This feature becomes more clear when compared with the method of common ownership of unsafe key shown in FIG.3. Referring to FIG.3, numeral 101 designates the first IC card, and numeral 102 designates the second IC card. The first IC card 101 comprises a random number generating means 103, a first enciphering means 104 and a second enciphering means 105. The second IC card 102 comprises a first decoding means 106 which is paired with the first enciphering means 104 and a second decoding means 107 which is paired with the second enciphering means 105. What is different from the embodiment of FIG.2 is that the first IC card 101 for transmitting a plain text m1 generates the random number r1, and sent it to the second IC card 102. In other words, the second IC card 102 performs the decoding process by using the random number r1 as a key which is sent from other party. In this method, the third party having the second IC card 102 decodes the r1 in own IC card by tapping the pair of the output of the first enciphering means 104 and the output of the second enciphering means 105, and input them into own IC card, and thereby the cipher text with respect to the plain text m1 can be deciphered. As mentioned above

BNSDOCID: <EP___0422230A1_I_>

by the method shown by FIG.3, safe common ownership of the key can not be realized.

From the above-mentioned fact, by the configuration of the IC card shown in FIG.2, the IC card which has generated the random number, namely only the second IC card 12 of the reception party is able to decode the cipher text, and it is understood that the cipher communication is safe. Moreover, if the IC card shown in FIG.2 is used, common ownership of the key is easily realizable since both the list of the secret keys and the center are not required. Additionally, since it is composed of only the secret key cipher, high speed processing is possible.

FIG.2 shows the case of a single direction communication, but in the event that both-direction communication is carried out, the configuration as shown in FIG.4 is preferable. Referring to FIG.4, numeral 21 designates the first IC card, numeral 22 designates the second IC card, and numerals 13 — 17 are identical with those of FIG.2, and the configuration are completely identical with FIG.2. In order to communicate in inverse direction of the embodiment of FIG.2, as other elements, the first IC card 21 comprises a second random number generating means 23, a third enciphering means 24, and a fourth decoding means 25. Moreover, the second IC card 22 comprises a third decoding means 26 which is paired with the third enciphering means 24, and a third enciphering means 27 which is paired with the fourth decoding means 25. The part which is composed of numerals 23 — 27 are symmetrical to the part which is composed of the numerals 13 — 17. Namely, when the second IC card 22 sent a plain text m2 to the first IC card 21, the first IC card 21 generates a random number r2 by using the second random number generating means 23, and it is enciphered by the third enciphering means 24 and is sent. The second IC card 22 decodes r2 which is enciphered by using the third decoding means 26 and r2 is obtained. After then, the first IC card 21 and the second IC card 22 perform the cipher communication of the plain text m2 by the fourth enciphering means 27 and the fourth decoding means 25 by using r2 as a session key.

Here, by using the same master key km that has been used when the random number r1 is enciphered as a key for enciphering and sending the random number r2, furthermore by using the same one which is to be applied on the same calculation to the first enciphering means 16 and the third enciphering means 24 (in a similar manner with respect to the decoding means 13 and 26 which are paired with them), and by using the same one which is to be applied on the same calculation to the second enciphering means 14 and the fourth enciphering means 27 (in a similar manner with respect to the decoding means 17, 25 which are paired with them), the first IC card 21 and the second IC card 22 become the same configuration except for the first random number generating means 15 and the second random number generating means 23. Namely, the communication parties which belong to the system carry out the cipher communication of both directions with an arbitrary communication party which belongs to this system by having each one IC card which has the same configuration. In this case, the first and the second random number generating means 15, 23 are preferable to output different random number series with respect to each IC card, but reference to this is minutely elucidated hereinafter.

Though each IC card comprises both the decoding means (13 or 26) for restoring the random number and the decoding means (25 or 17) for restoring the message, in a similar manner to the embodiment of FIG.2, deciphering of the cipher text which is directed to other person is impossible, and safety of the cipher communication is maintained since an arbitrary establishment of the decoded key and decoding processing by using the key can not be carried out simultaneously by using own IC card.

FIG.5 is a block diagram showing other embodiment of the IC card of the present invention. Referring to FIG.5, numeral 31 designates the first IC card, numeral 32 designates the second IC card. The first IC card 31 comprises a first exclusive logical sum calculation means 33, a first enciphering means 34, a second random number generating means 35, a second exclusive logical sum calculation means 36, and a second decoding means 37. And, the second IC card 32 comprises a first random number generating means 38, a third exclusive logical sum calculation means 39, a first decoding means 40 which is paired with the first enciphering means 34, a fourth exclusive logical sum calculation means 41, and a second enciphering means 42 which is paired with the second decoding means 37. Here, the first enciphering means 34 and the second enciphering means 42 perform the same calculation (it is the similar with respect to the decoding means 40, 37 which are paired with them). The present embodiment is identical with the embodiment of FIG.4, and shows the case which performs bilateral communication, and the first IC card 31 and the second IC card 32 have entirely the same configuration except for the random number generating means 38, 35.

Hereafter, according to FIG.5, operation of the present embodiment is elucidated. First, the case in that the first IC card 31 sends a plain text m1 to the second IC card 32 is elucidated. The second IC card 32 sends the random number r1 which is generated by the first random number generating means 38 to the first IC card 31. The first IC card 31 and the second IC card 32 perform exclusive logical sum calculation of the random number r1 and the master key km by using a first exclusive logical sum calculation means 33

BNSDOCID: <EP___0422230A1_I_>

and the third exclusive logical sum calculation means 39, respectively, and a session key ksl is obtained. The master key km is common to the whole IC cards. Hereafter, the first IC card 31 and the second IC card 32 carry out cipher communication of the plain text m1 by using the session key which is common to both the parties. In the case where the second IC card 32 sends a plain text m2 to the first IC card 31 is also carried out in the same manner by generation of a random number r2 by the first IC card 31 using the second random number generating means 35.

Safety of the embodiment, similarly with the embodiment of FIG.2 and FIG.4, is assured by that arbitrary setting of the decoding by using own IC card and the decoding processing by using the key can not be carried out simultaneously.

However, in the above-mentioned example, since the whole communicating parties which belong to the system have the card of the same configuration, pretending as other person is possible. An example of an IC card which is added with a function for certifying such other person in order to prevent this, is shown in FIG.6. Referring to FIG.6, numeral 51 designates the first IC card, and numeral 52 designates the second IC card. The first IC card 51 comprises first exclusive logical sum calculation means 53, a first enciphering means 54, a second random number generating means 55, a second key generating means 56, a second exclusive logical sum calculation means 57 and a second decoding means 58. Moreover, the second IC card 52 comprises a first random number generating means 59, a first key generating means 60, a third exclusive logical sum calculation means 61, a first encoding means 62 which is paired with the first enciphering means 54, a fourth exclusive logical sum calculation means 63, and a second enciphering means 64 which is paired with the second decoding means 58. Where, the first enciphering means 54 and the second enciphering means 64 perform the same calculation (the decoding means 62, 58 which are paired with them are identically performed). Additionally, the first key generating means 60 and the second key generating means 56 perform the same calculation. In a manner similar to the embodiment of FIG.4 and FIG.5, though the present embodiment shows the case performing both directions communication, the first IC card 51 and the second IC card 52 have card identifying information (IDa, IDb) and secret keys (Ka, Kb) which are different from each card, respectively.

Hereafter, operation of the present embodiment is elucidated in compliance with FIG.6. First, the case in which the first IC card 51 sends a plain text m1 to the second IC card 52 is elucidated. The second IC card 52 sends the random number r1 which is generated by the first random number generating means 59 to the first IC card 51. On the other hand, the first IC card 51 sends own card identifying information IDa to the second IC card 52. The second IC card 52 performs calculation by using the card identifying information IDa which is sent from the other party and the master key km as parameters. Here, relation between the card identifying information and the secret key of whole IC cards is set in each IC card at the time of publication so as to satisfy that

Secret key = F (card identifying information, km)

F: Function of key generating means

km: a master key which is common to whole IC card.

Consequently, the result of the above-mentioned calculation is

ka = F (IDa, km), and

thus, the secret key of the first IC card 51 is generated in the second IC card 52. Subsequently, the first IC card 51 and the second IC card 52 carry out exclusive logical sum calculation of the random number r1 and the secret key ka by using the first exclusive logical sum calculation means 53 and the third exclusive logical sum calculation means 61, respectively, and the session key ksl is obtained. After then, the first IC card 51 and the second IC card 52 carry out cipher communication of a plain text m1 by using the session key ksl which is common to both parties. The case that the second IC card 52 sends a plain text m2 to the first IC card 51 can be performed in the same manner by that the first IC card 51 generates the random number r2 by using the second random number generating means 55 and the second IC card 52 sends own card identifying information IDb to the second IC card 51.

Safety of the present embodiment is assured in a manner similar to the above-mentioned embodiments, because an arbitrary setting of the decoding key by using one's own IC card and decoding processing by using the key can not be simultaneously carried out. Further, in the present embodiment, even if an evil-minded third party pretends as the owner of the first IC card 51 and sends IDa to the second IC card 52, a message making sense can not be sent by enciphering, since only the first IC card 51 has the secret key ka, for example. Therefore, fraud due to "pretending" can be easily seen through by a suitable protocol.

Safety of the embodiments hitherto described mainly depends on the structure of the random number generating means. Namely, if the random number which is generated by own IC card can be manipulated, or the random number system can be predicted, the evil-minded person is capable of deciphering the tapped cipher text by using own IC card. For example, if the random number generating means has a

BNSDOCID: <EP___0422230A1_I_>

structure bringing the input from the outside into a parameter, a necessary random number can be generated in own IC card. Moreover, if the random number system is common to whole IC cards, the random number which is automatically generated in the inside of own IC card can be anticipated by investigating the random number system of an IC card. On the basis of this aspect, a safe random number generating means which is impossible to be manipulated from the outside and generates a random number system which is different from each IC card is shown in FIG.7.

FIG.7 is a block diagram of the random number generating means, and numeral 72 designates a non-volatile memory which is capable of electric rewriting, numeral 73 designates an adder, and numeral 74 designates enciphering means. The non-volatile memory 72 stores data of 64 bits, for example. The adder 73 adds 1 to the 64 bits data which is stored in the non-volatile memory 72, and omits the overflow part and generates the 64 bits data. The 64 bits data is inputted to the enciphering means 74, simultaneously is fed back to input for the subsequent calculation by the adder 73, and is stored in the non-volatile memory 72. The enciphering means 74 enciphers the 64 bit data which is output from the adder 73 by the key which is peculiar to each IC card and outputs. As the key which is peculiar to each IC card, for example the secret keys ka, Kb shown in the embodiment of FIG.6 are usable.

Here, if the output of the adder 73 has a long period, the output value of the enciphering means 74 becomes an enough random value. Moreover, since an output from the outside is not used at all, even the owner of the IC card can not manipulate the output of the random number generating means. Furthermore, the key of the enciphering means 74 is a peculiar value to each IC card, and hence even if the random number generating means of whole IC cards has the same configuration, the output random number system is different from each IC card.

FIG.8 is a block diagram of an IC card in accordance with other embodiment of the present invention. Referring to FIG.8, numeral 211 designates a first IC card, and numeral 212 designates a second IC card, and in order to hold in common a common key and the like, the first IC card 211 comprises a first random number generating means 213, a first enciphering means 214 and a second decoding means 215, and the second IC card 212 comprises a second random number generating means 216, a first decoding means 217 which is paired with the first enciphering means 214, and a second enciphering means 218 which is paired with the second encoding means 215. And, in order to send a message from the first IC card 211, the first IC card 211 comprises a third enciphering means 219, a first register 220 and a first exclusive logical sum calculation means 221. Moreover the second IC card 212 comprises a third decoding means 222 which is paired with the third enciphering means 219, a second register 223 and a second exclusive logical sum calculation means 224. Furthermore, in order to send a message from the second IC card 212, the first IC card 211 comprises a fourth decoding means 225, a third register 226 and a third exclusive logical sum calculation means 227. Furthermore, the second IC card 212 comprises a fourth enciphering means 227 which is paired with the fourth decoding means 225 and a fourth register 229 and a fourth exclusive logical sum calculations means 230.

Hereafter, operation of the present embodiment is elucidated, in compliance with FIG.8. First, the first IC card 211 enciphers the first random number r1 output from the first random number generating means 213 by a master key km by using the first enciphering means 214 and sent to the second IC card 212. The second IC card 212 decodes the enciphered random number by the master key km and restores the first random number r1 by using the first decoding means 217. Moreover, the second IC card 212 enciphers the second random number r2 output from the second random number generating means 216 by the master key km by using the second enciphering means 218 and sends to the first IC card 211. The first IC card 211 decodes the enciphered random number by the master key km and restores the second random number r2 by using the second decoding means 215. By the process as has above-mentioned, the first IC card 211 and the second IC card 212 result in holding two common secret random numbers r1, r2 in common.

Subsequently, a method for sending a message from the first IC card 211 to the second IC card 212 by using r1, r2 which are held in common is elucidated. In the following elucidation, a sign "+" means exclusive logical sum calculation. First, at start of the cipher communication, as an initial state, the first random number r1 is stored in the first and second registers 220, 223. The first IC card 211 divides the message of the plain text to be sent into respective ciphering units. Plural blocks which are obtained as mentioned above, are named as m1, m2, m3. The third enciphering means 219 applies a ciphering process to the head block m1 by using the second random number r2 as a key, and as a result c1 = E3r2(m1) is output to the first exclusive logical sum calculation means 221. Here, E3 shows a cipher function of the third ciphering means 219. The first exclusive logical sum calculation means 221 calculates an exclusive logical sum of the input c1 from the enciphering means 219 and the data (initial value r1) in the first register 220, and sends the result c1 + r1 to the second IC card 212.

BNSDOCID: <EP___0422230A1_I_>

On the other hand, in the following manner, the second IC card 212 restores the plain text m1 from received data (cipher text) c1 + r1. The second IC card 212 calculates an exclusive logical sum of the above-mentioned data c1 + r1 which is sent and the data (initial value r1) in the second register 223, and as a result (c1 + r1) + r1 = c1 is output to the third decoding means 222. The decoding means 222 applies the decoding process to the above-mentioned data c1 = E3r2(m1) which is sent by using the second random number r2 as a key, and restore the result m1. Thereafter, the first IC card 211 stores the plain text m1 in the first register 220 as a replacement for the initial value r1, on the one hand, the second IC card 212 stores the restored plain text m1 in the second register 223 as a replacement for the initial value r1. Therefore, the first IC card 211 and the second IC card 212 hold in common the r1 and r2, and as far as the data in communication is not varied accidentally or with intention, the same value is always stored in the first register 220 and the second register 223. All the plain text can be restored by repeating the above-mentioned same process of the head block m1 to m2, m3.

In the event that the plain text m4, m5, m6 are sent from the second IC card 212, the cipher communication can be carried out in a similar manner by using the fourth decoding means 226, the third register 226, the third exclusive logical sum calculation means 227, the fourth enciphering means 228, the fourth register 229 and the fourth exclusive logical sum calculation means 230. The data value at each important point in this case is shown in the following Table 1. The sign "+" in the Table 1 shows exclusive logical sum calculation.

Table 1

The case of transmission of a message from the second IC card in FIG.8

Second IC card 212			First IC card 211	
Normal sentence	Fourth register	Sending and receiving data	Third register	Restored sentence
m4	r1	E4r2 (m4) + r1	r1	m4
m5	m4	E4r2 (m5) + m4	m4	m5
m6	m5	E4r2 (m6) + m5	m5	m6

The reason why the present embodiment is safe is elucidated hereafter. First, since the master key km is stored in the memory in the IC card which is physically safe, even the owner of the IC card can not read out the master key km. Therefore, even if the output of the first enciphering means 214 and the output of the second enciphering means 218 are tapped on the communication line, the first random number r1 and the second random number r2 can not be restored without using the IC card in which the master key km is stored. Consequently, deciphering of the cipher text is impossible.

Subsequently, a case is considered that there are three communication parties A, B, C which belong to this system and C intends to decipher the cipher text which is exchanged between A and B. Since C is the communicating party which belongs to this system, C has the first IC card 211 or the second IC card 212. First, it is assumed that C has the second IC card 212, and intends to decipher the cipher text from the first IC card 211. In this case, even if C taps the cipher text which is sent from the first IC card 211 (namely, the output of the first exclusive logical sum calculation means 221) and inputs it to his own IC card, the tapped cipher text can not be decoded correctly since the decoding key of the third decoding means 222 is not the second random number r2 but a random number which is automatically generated in the IC card in that time.

Subsequently, it is assumed that C has the first IC card 211, and intends to decipher the cipher text from the second IC card 212. In this case, the second random number r2, namely the decoding key of the fourth decoding means 225 can be generated in his own IC card by the second decoding means 215 and the master key km, by that C taps the output of the second enciphering means 218 which is exchanged between A and B (namely, enciphered second random number), and input it to his own IC card. However, in

BNSDOCID: <EP___0422230A1_I_>

this time, the IC card of C can not correctly decode the cipher text from the second IC card 212, since the IC card automatically generates a random number inside by the first random number generating means 213 (this random number is r3), and bring it to an initial value of the third register 226. The state is shown in the following Table 2. From Table 2, first, it is understood that the m1 is not correctly decoded, since r1 ≠ r3. Since m1 which is not correctly decoded is fed back to the third register 226, successive m2 is not also correctly decoded. In this way, influence of r1 ≠ r3 is given to all successive data thereto, and deciphering of the cipher text which is output from the second IC card 212 become completely impossible.

Table 2

The case that the initial value of the register differs in FIG.8

Second IC card 212			First IC card 211	
Normal sentence	Fourth register	Sending and receiving data	Third register	Restored sentence
m4	r1	E4r2 (m4) + r1	≠r1	≠m4
m5	m4	E4r2 (m5) + m4	≠m4	≠m5
m6	m5	E4r2 (m6) + m5	≠m5	≠m6

The feature of the present invention is further clarified by comparison with the unsafe cipher communicationsystem shown in FIG.9. FIG.9 shows a block diagram of an IC card which performs unsafe cipher communication, and numeral 281 designates a first IC card, numeral 282 designates a second IC card. All structural elements and the configuration of 213 — 224 are completely identical with FIG.8, but as to 225 — 230, the point that the second IC card 212 has a feed-back function and the first IC card 211 has a feed-forward function, is inverted to the case of FIG.8.

In this configuration, the case in which the third party C having the first IC card 281 attempts to decipher the cipher text which is output from the second IC card 282 is considered. As mentioned above, C can generate the second random number r2 by tapping the output of the second enciphering means 218 and by inputting it in his own IC card. At the same time, the IC card of C automatically generates the random number r3 which is different from the first random number r1. By using r2 as the decoding key, and by using the r3 as an initial value of the third register 226, the data value of each important point in the case which attempts to decipher the cipher text from the second IC card 282 is shown in the following Table 3. As is understood from the Table 3, although the head block is just impossible to be deciphered, the influence does not affect after then since the receiving side has no feed-back function, and deciphering is made possible after the second block. In the system shown in FIG.9 as this way, safe cipher communication is not realized.

BNSDOCID: <EP___0422230A1_I_>

Table 3

The case in which the initial value of the register differs in FIG.9

Second IC card 282			First IC card 281	
Normal sentence	Fourth register	Sending and receiving data	Third register	Restored sentence
m4	r1	c4 = E4r2 (m4+r1)	≠r1	≠m4
m5	c4	c5 = E4r2 (m5+c4)	c4	m5
m6	c5	c6 = E4r2 (m6+c5)	c5	m6

As is understood from the above, by the configuration of the IC card shown in FIG.8, the IC card which can have both the first random number r1 and the second random number r2, namely only the IC card of the party concerned which performs cipher communication is made possible to decipher the cipher text, and the cipher communication is secured. And, by using the IC card shown in FIG.8, common ownership of the key is easily realized since both the list of the secret keys and the center are not necessary. Moreover, since it can be structured by only the secret key cipher, high speed processing is realizable.

And, the first IC card 211 and the second IC card 212 becomes completely the same configuration except for the first random number generating means 213 and the second random number generating means 216, by using one for applying the same calculation to the first enciphering means 214 and the second enciphering means 218 (which is identical with respect to the decoding means 217, 215 which are paired with them), and furthermore by using one for applying the same calculation to the third enciphering means 219 and the fourth enciphering means 228 (which is identical with respect to the decoding means 222, 225 which are paired with them). Namely, the communication parties which belong to this system can do bilateral directions cipher communication with an arbitrary communication party which belongs to this system by respectively having one IC card of the same structure. In this case, the random number generating means 213, 216 are preferable to output a random number system which differs from each IC card.

FIG.10 is a block diagram of the IC card with an enciphering processing function in accordance with other embodiment of the present invention. Referring to FIG.10, numeral 251 designates a first IC card, numeral 252 designates a second IC card; and the first IC card 251 comprises a first random number generating means 253, a fifth exclusive logical sum calculation means 254, a sixth exclusive logical sum calculation means 225 for holding in common a key and an initial value of a register; and the second IC card 252 comprises a second random number generating means 256, a seventh exclusive logical sum calculation means 257 and a eighth exclusive logical sum calculation means 258. The structural elements 219 ---230 for performing cipher communication of a message and the configuration are completely identical with the embodiment of FIG.8.

Hereafter, in compliance with FIG.10, operation of the present embodiment is elucidated. The first IC card 251 sends the first random number r1 which is generated by the first random number generating means 253 to the second IC card 252, in order to hold in common the key and the initial value of the register. The first IC card 251 and the second IC card 252 perform exclusive logical sum calculation of the random number r1 and the master key km by using the fifth exclusive logical sum calculation means 254 and the seventh exclusive logical sum calculation means 257, respectively, and a common key ks is obtained. In the similar manner, a common initial value I is obtained in the registers 220, 223, 226 and 229 by using the second random number generating means 256 and the sixth exclusive logical sum calculation means 255 and the eighth exclusive logical sum calculation means 258. The method of cipher communication thereafter and safety of the present embodiment are completely identical with the embodiment of FIG.8 and thus the elucidation is omitted.

BNSDOCID: <EP___0422230A1_I_>

INDUSTRIAL APPLICABILITY

As mentioned above, according to the present invention, common ownership of a key for cipher communication is safely, easily and speedily realizable by storing a secret key in an IC card which is physically safe and generating a decoding key from a random number of which the IC card of a reception party automatically output and generating an enciphering key from the random number which is sent from the reception party. Moreover, in comparison with the conventional key common ownership system using the secret key cipher, the present invention has a very useful feature in practical use by which common ownership of the key is realizable without requiring both the list of the secret keys and a key distribution (or translation) center. Moreover, since it is realizable with only the secret key cipher, it is superior in the aspect of a processing speed which is required for ciphering and decoding to the method of the conventional cipher communication using a public key cipher.

Furthermore, by making that all IC cards which are used in one system are made by the same configuration except for a card identifying information and the secret key which are peculiar to each IC card, in the aspect of operation, bilateral directions communication is realizable with an arbitrary communication party which belongs to the system; and on the other hand in the aspect of fabrication, mass-production of the IC card is made possible, and the effect in its practical use is very large.

List of reference numerals of figures

1	First terminal
2	Second terminal
3	First IC Card
4	Cipher apparatus
5	Second IC Card
6	Decoding apparatus
7	Input apparatus
8	Transmission apparatus
9	Output apparatus
10	Reception apparatus
11	First IC card
12	Second IC card
13	First decoding means
14	Second enciphering means
15	Random number generating means
16	First enciphering means
17	Second decoding means
21	First IC card
22	Second IC card
23	Second random number generating means
24	Third enciphering means
25	Fourth decoding means
26	Third decoding means
27	Fourth enciphering means
31	First IC card
32	Second IC card
33	First exclusive logical sum calculation means
34	First enciphering means
35	Second random number generating means
36	Second exclusive logical sum calculation means
37	Second decoding means
38	First random number generating means
39	Third exclusive logical sum calculation means
40	First decoding means
41	Fourth exclusive logical sum calculation means
42	Second enciphering means
43	Random number generating means
44	First enciphering means
45	Second enciphering means
46	First decoding means

BNSDOCID: <EP___0422230A1_I_>

47 Second decoding means
51 First IC card
52 Second IC card
53 First exclusive logical sum calculation means
54 First enciphering means
55 Second random number generating means
56 Second key generating means
57 Second exclusive logical sum calculation means
58 Second decoding means
59 First random number generating means
60 First key generating means
61 Third exclusive logical sum calculation means
62 First decoding menas
63 Fourth exclusive logical sum calculation means
64 Second enciphering means
72 Non-volatile memory
73 Adder
74 Enciphering means
101 First IC card
102 Second IC card
103 Random number generating means
104 First enciphering means
105 Second enciphering means
106 First decoding means
107 Second decoding means
211 First IC card
212 Second IC card
213 First random number generating means
214 First enciphering means
215 Second decoding means
216 Second random number generating means
217 First decoding means
218 Second enciphering means
219 Third enciphering means
220 First register
221 Flrst exclusive logical sum calculation means
222 Thirs decoding means
223 Second register
224 Second exclusive logical sum calculation means
225 Fourth decoding means
226 Third register
227 Third exclusive logical sum calculation means
228 Fourth enciphering means
229 Fourth register
230 Fourth exclusive logical sum calculation means
253 First random number generating means
254 Fifth exclusive logical sum calculation means
255 Sixth exclusive logical sum calculation means
256 Second random number generating means
257 Seventh exclusive logical sum calculation means
258 Eighth exclusive logical sum calculation means
281 First IC card
282 Second IC card

Claims

1. A data carrier comprising: means for holding inside data which is impossible to be changed to data

BNSDOCID: <EP___0422230A1_I_>

which is designated from outside, enciphering means for enciphering said inside data by a secret key and outputting to outside, and decoding means for decoding a cipher text which is inputted from outside by said inside data.

2. A data carrier comprising: decoding means for decoding enciphered data which is inputted from outside by a secret key and enciphering means for enciphering plain text which is inputted from outside or is stored inside by the output of said decoding means and for outputting to outside.

3. A data communication apparatus having configuration that, a first terminal and a second terminal for performing communication with this first terminal are comprised, said first terminal comprising an input apparatus, an enciphering apparatus for enciphering the data inputted from this input apparatus and a transmission apparatus for transmitting the data which is enciphered by this enciphering apparatus to said second terminal, said second terminal comprising a reception apparatus for receiving the data which is sent from said transmission apparatus and a decoding apparatus for decoding the data which is received by this reception apparatus, said enciphering apparatus and decoding apparatus being provided in said first data carrier which is loaded in said first terminal and in the second data carrier which is loaded in said second terminal, respectively, and said decoding apparatus comprising means for holding the inside data which is impossible to be changed to data which is designated from outside, a first enciphering means for outputting to the enciphering apparatus of said first data carrier and second decoding means for decoding the cipher text which is inputted from said enciphering apparatus of said first data carrier by said inside data, said enciphering apparatus comprising first decoding means for decoding enciphered data which is inputted from said first enciphering means by a secret key, and second enciphering means for enciphering plain text which is inputted from outside or is stored inside by output of said first decoding means and for outputting to said second decoding means of said decoding apparatus.

4. A data carrier comprising, means for holding inside data which is impossible to be changed to the data which is designated from the outside, calculation means for applying calculation to this inside data by using a secret parameter, and decoding means for decoding the cipher text which is inputted from outside by the output of said calculation means.

5. A data carrier in accordance with claim 4 characterized in that, said calculation means comprises key generating means for applying calculation to identifying information of a communication party which is inputted from outside by using said secret parameter, and calculation means for applying calculation to said output of this key generating means by using said inside data.

6. A data carrier comprising, calculation means for applying calculation to data which is inputted from outside by using a secret parameter, and enciphering means for enciphering a plain text which is inputted from outside or is stored inside by said output of said calculation means.

7. A data communication apparatus having configuration that, a first terminal and a second terminal which performs communication with this first terminal are comprised, said first terminal comprising an input apparatus and an enciphering apparatus for enciphering data inputted from this input apparatus, and a transmission apparatus for transmitting data which is enciphered by this enciphering apparatus toward said second terminal, said second terminal comprises a reception apparatus for receiving data sent from said transmission apparatus and a decoding apparatus for decoding data received by this reception apparatus, said enciphering apparatus and a decoding apparatus are provided in said first data carrier loaded to a first terminal and in said second data carrier loaded in the second terminal, respectively, and said decoding apparatus comprises means for holding inside data which is impossible to be changed to data which is designated from the outside, first calculation means for applying calculation to this inside data by using a secret parameter, and first decoding means for decoding the cipher text which is inputted from enciphering apparatus of said first data carrier by output of said first calculation means, and said enciphering apparatus comprises second calculation means for applying calculation to the inside data which is inputted from said decoding apparatus by using a secret parameter, and first enciphering means for enciphering a plain text which is inputted from outside or is stored inside by output of said second calculation means, and output to the first decoding means of said decoding apparatus.

BNSDOCID: <EP___0422230A1_I_>

8. A data carrier having configuration that, means for holding inside data which is impossible to be changed to the data which is designated from outside, an enciphering means for enciphering this inside data by a secret key and output to outside, exclusive logical sum calculation means for performing exclusive logical sum calculation of the cipher text which is inputted from outside and the data which is stored in a register, and a decoding means for decoding output of this exclusive logical calculation means are provided, and at start of encipher communication said inside data or the same thereto is stored in said register, and after finish of decoding process by said decoding means output of said decoding means is stored in said register.

9. A data carrier having configuration that, decoding means for decoding enciphered data which is inputted from outside by a secret key, enciphering means for enciphering a plain text which is inputted from outside or is stored inside, and exclusive logical sum calculation means for performing exclusive logical sum calculation of the output of this enciphering means and the register are provided, and at start of cipher communication output of said decoding means is stored in said register, and after finish of the calculation process by said exclusive logical sum calculation means, said plain text is stored in said register.

10. A data carrier having configuration that, means for holding inside data which is impossible to be changed to the data which is designated by outside, calculation means for applying calculation to said inside data by using a secret parameter, and exclusive logical sum calculation means for performing exclusive logical sum calculation of the cipher text which is inputted from the outside and the data which is stored in the register are provided, and at the start of cipher communication, the output of said calculation means is stored in said register, and after finish of decoding process by said decoding means, the output of said decoding means is stored in said register.

11. A data carrier in accordance with claim 10, wherein said calculation means is exclusive logical sum calculation means.

12. A data carrier having configuration that, calculation means for applying calculation to the data which is inputted from outside by using a secret parameter, enciphering means for enciphering a plain text which is inputted from outside or is stored inside, and exclusive logical sum calculation means for performing exclusive logical sum calculation of the output of this enciphering means and a register are provided, at the start of cipher communication, output of said calculation means is stored in said register, and after finish of calculation process by said exclusive logical sum calculation said plain text is stored in said register.

13. A data carrier in accordance with claim 12, wherein calculation mean is exclusive logical sum calculation means.

BNSDOCID: <EP___0422230A1_I_>

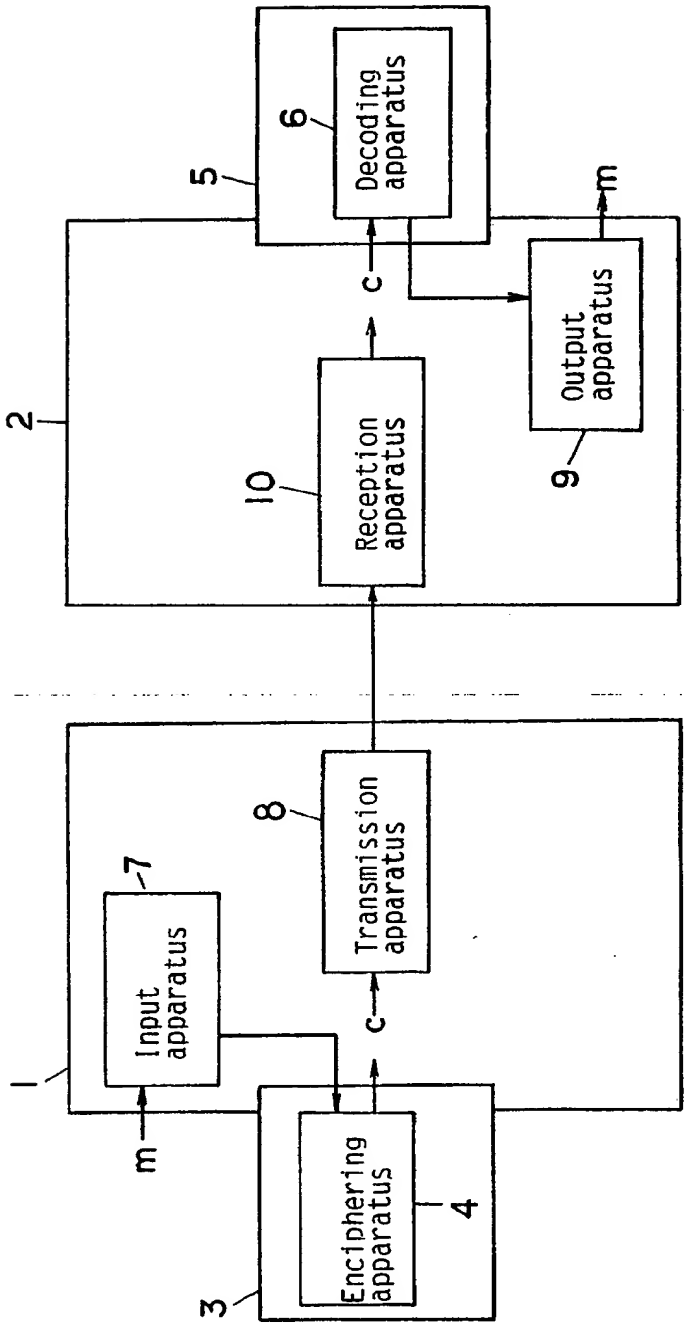
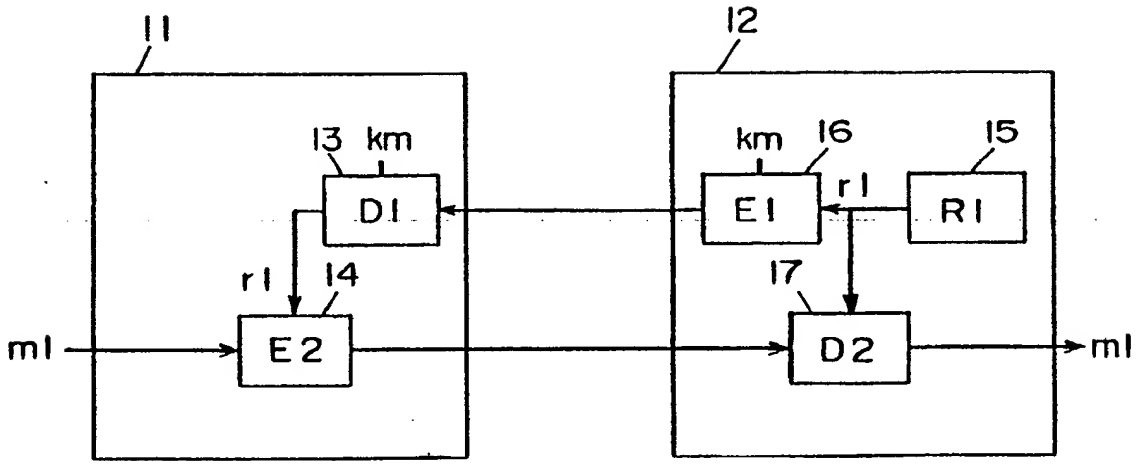

Decoding apparatus
6
5
m
c
Output apparatus
9
2
Reception apparatus
10
Transmission apparatus
8
7
Input apparatus
c
1
m
Enciphering apparatus
4
3

FIG. 1

FIG. 2



BNSDOCID: <EP___0422230A1_I_>

FIG. 3

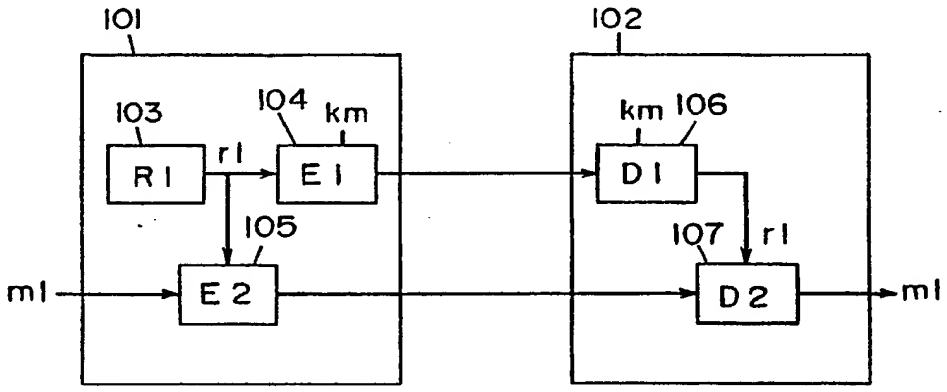
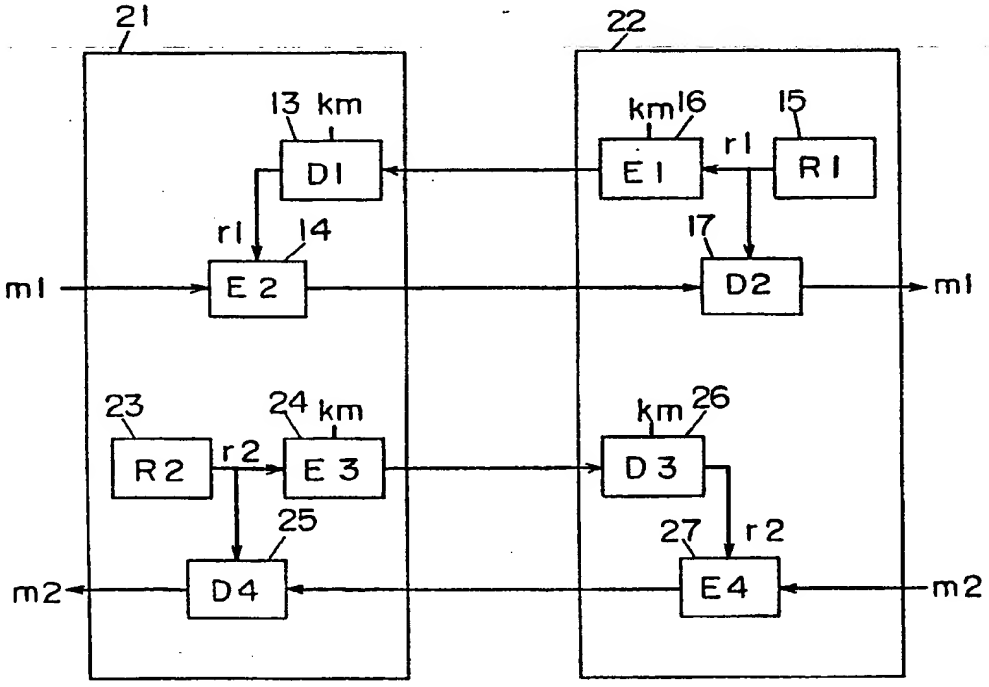
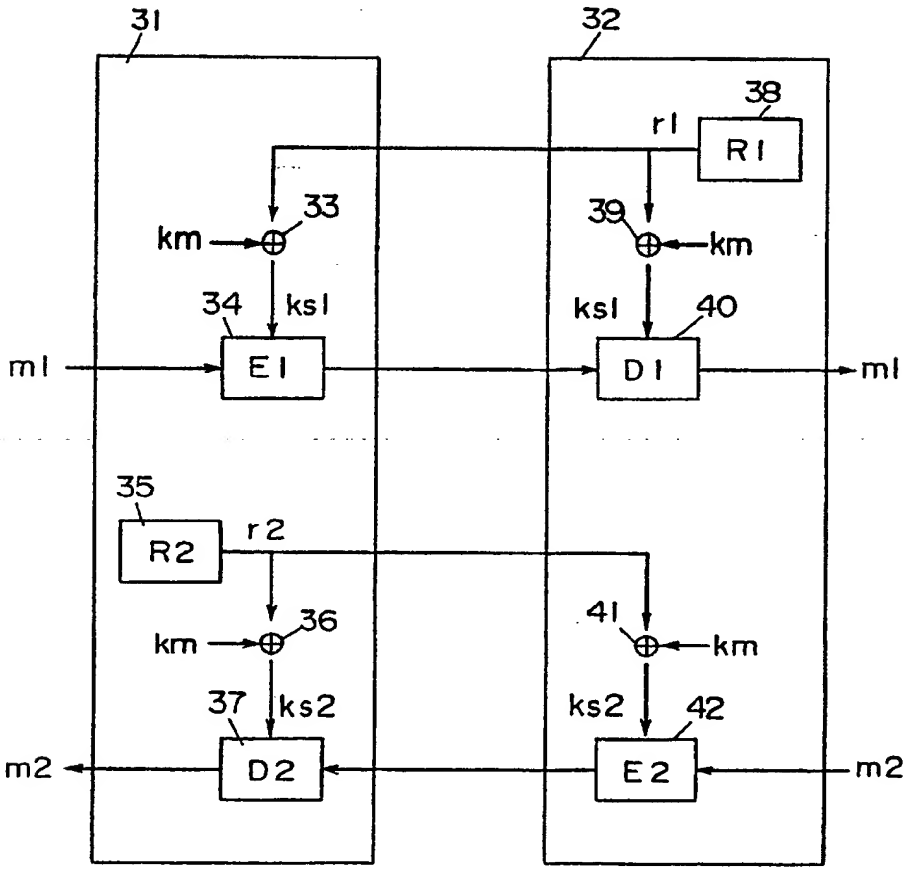


FIG. 4



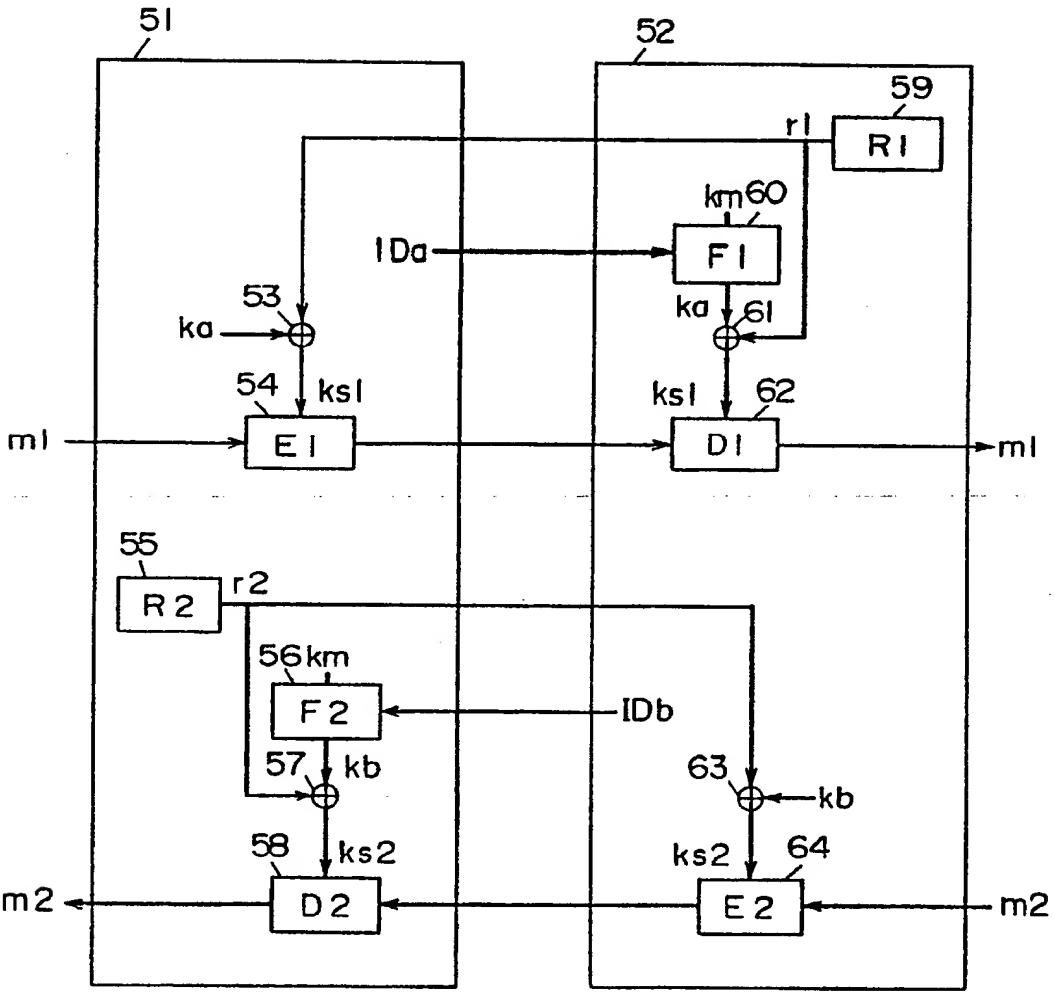
BNSDOCID: <EP___0422230A1_I_>

FIG. 5



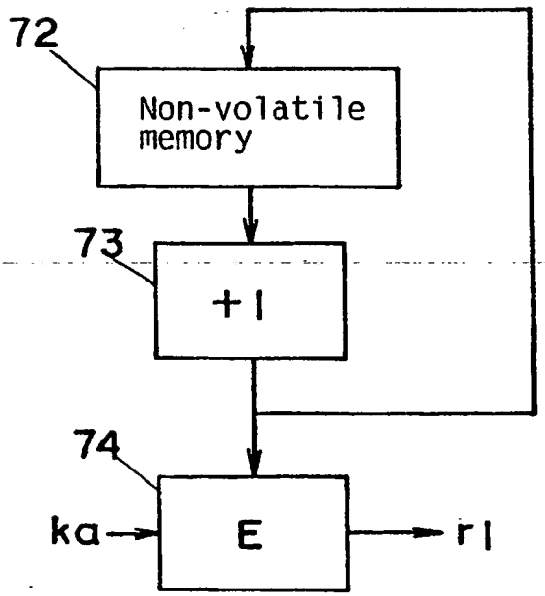
BNSDOCID: <EP___0422230A1_I_>

FIG. 6



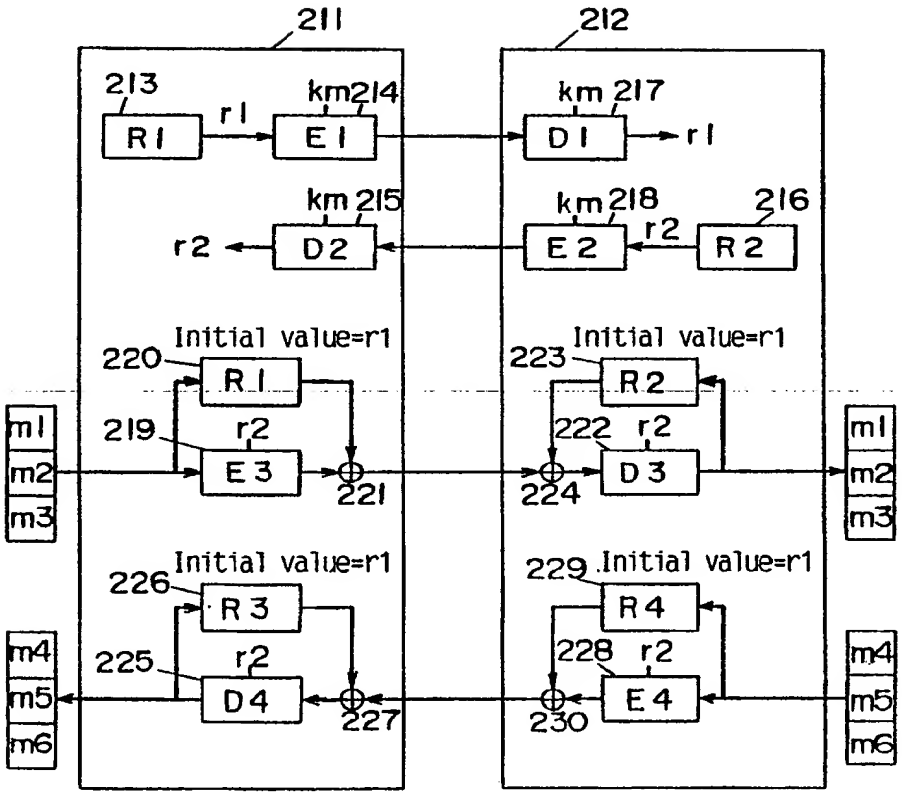
BNSDOCID: <EP___0422230A1_I_>

FIG. 7



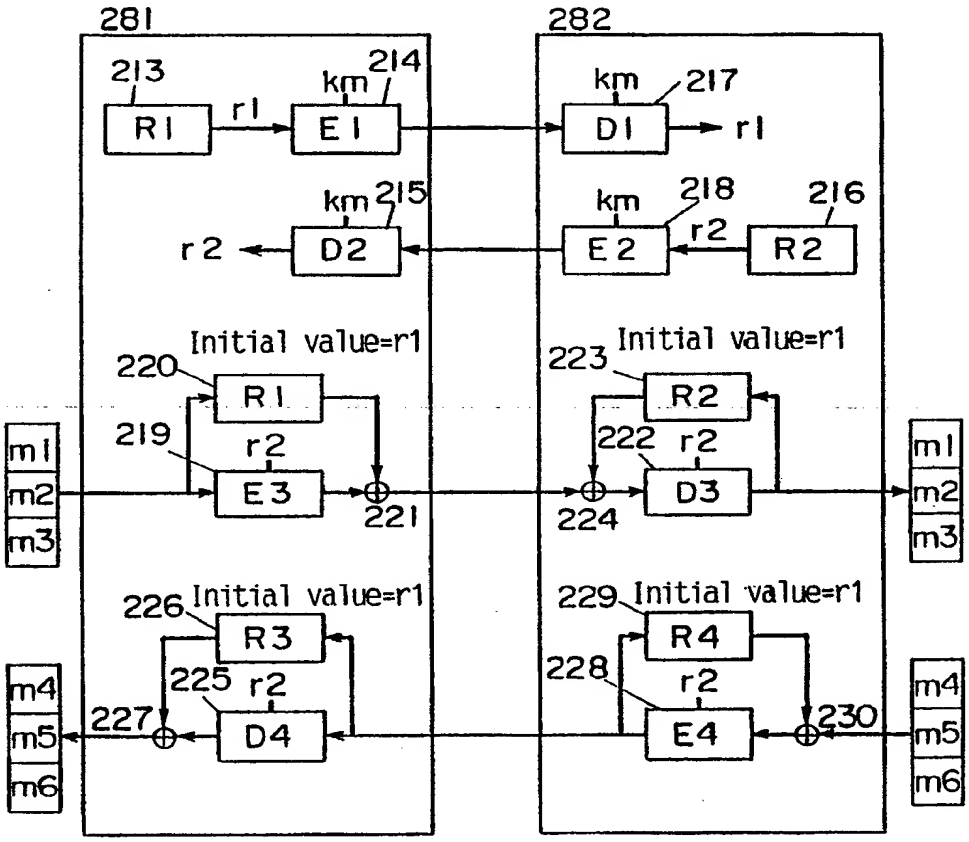
BNSDOCID: <EP___0422230A1_I_>

FIG. 8



BNSDOCID: <EP___0422230A1_I_>

FIG. 9



BNSDOCID: <EP___0422230A1_I_>

FIG. 10

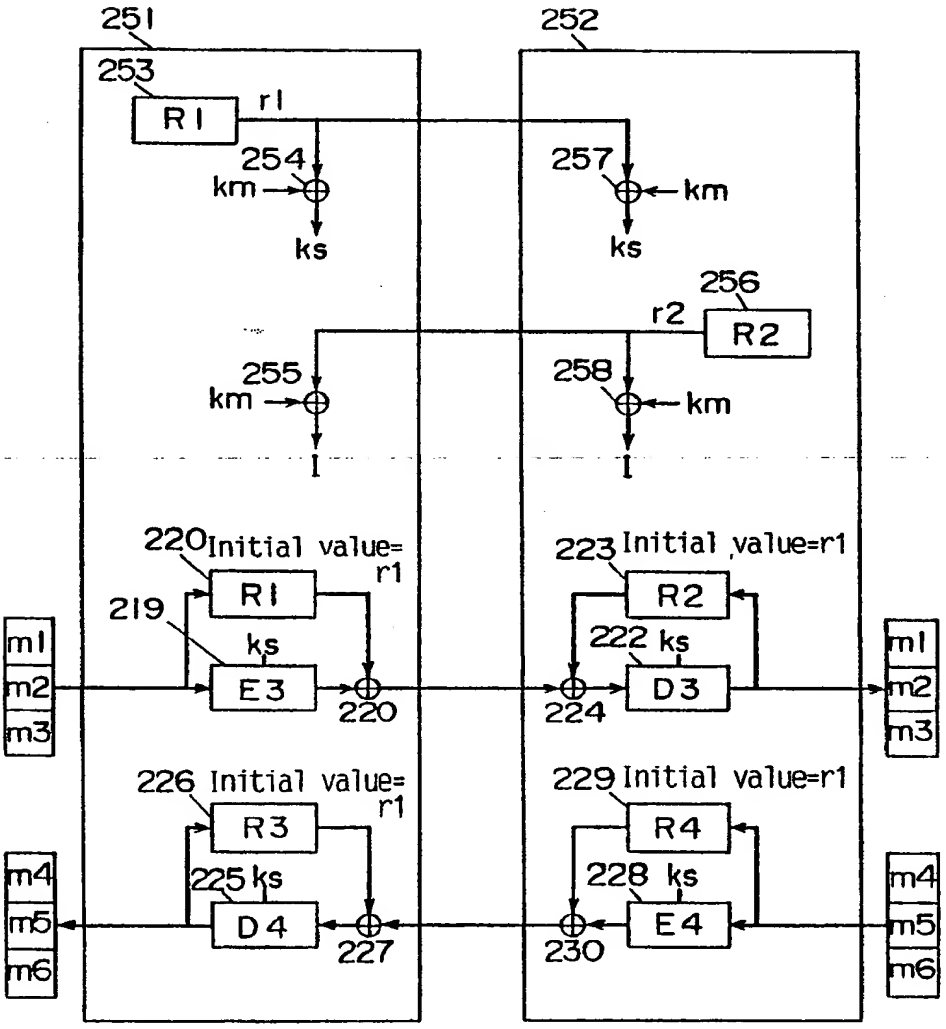
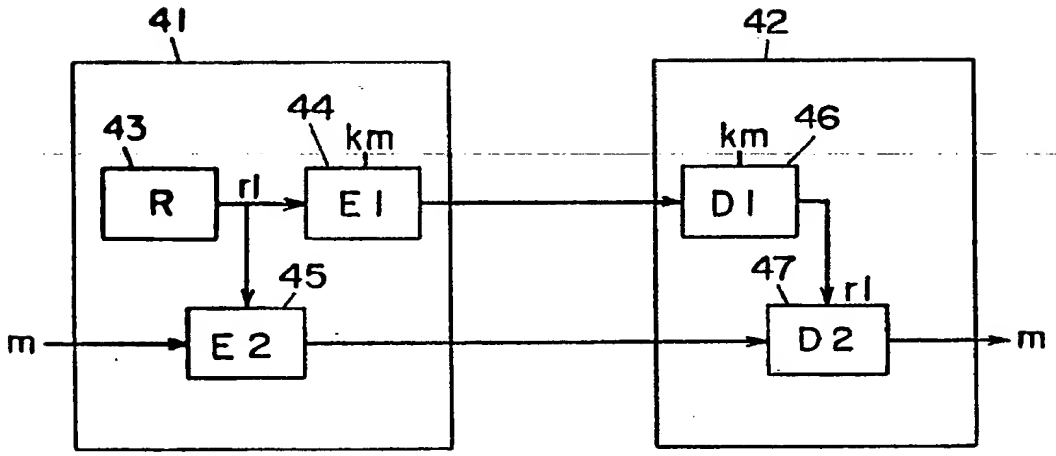

251
252
253
R1
r1
254
km
ks
257
km
ks
256
r2
R2
255
km
I
258
km
I
220 Initial value= r1
R1
219
ks
E3
220
223 Initial value=r1
R2
222 ks
D3
224
m1
m2
m3
226 Initial value= r1
R3
225 ks
D4
227
229 Initial value=r1
R4
228 ks
E4
230
m4
m5
m6

FIG. 11



BNSDOCID: <EP___0422230A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No PCT/JP90/00078

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl^5 G06K19/073, 17/00, G09C1/00

II. FIELDS SEARCHED

Minimum Documentation Searched *

Classification System	Classification Symbols
IPC	G06K19/073, 17/00, G09C1/00

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched *

Jitsuyo Shinan Koho	1971 - 1988
Kokai Jitsuyo Shinan Koho	1971 - 1988

III. DOCUMENTS CONSIDERED TO BE RELEVANT *

Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages **	Relevant to Claim No. **
A	JP, A, 60-62252 (Toshiba Corp.), 16 September 1985 (16. 09. 85), & EP, A, 138,386	1 - 13
A	JP, A, 62-189593 (Hitachi, Ltd.), 19 August 1987 (19. 08. 87), (Family: none)	1 - 13
A	JP, A, 62-191991 (NEC Corporation), 22 August 1987 (22. 08. 87), (Family: none)	1 - 13
A	JP, A, 63-50222 (Matsushita Electric Ind. Co., Ltd.), 3 March 1988 (03. 03. 88), (Family: none)	1 - 13
A	JP, A, 63-131169 (Hitachi, Ltd.), 3 June 1988 (03. 06. 88), (Family: none)	1 - 13

* Special categories of cited documents: **

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
April 3, 1990 (03. 04. 90)	April 16, 1990 (16. 04. 90)
International Searching Authority	**Signature of Authorized Officer**
Japanese Patent Office	

Form PCT/ISA/210 (second sheet) (January 1985)

BNSDOCID: <EP___0422230A1_I_>

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

A	JP, A, 63-219244 (Matsushita Electric Ind. Co., Ltd.), 12 September 1988 (12. 09. 88), (Family: none)	1 - 13

V. ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [1]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons.

1. ☐ Claim numbers , because they relate to subject matter not required to be searched by this Authority, namely.

2. ☐ Claim numbers , because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim numbers , because they are dependent claims and are not drafted in accordance with the second and third sentences of PCT Rule 6.4(a).

VI. ☐ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [2]

This International Searching Authority found multiple inventions in this international application as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

4. ☐ As all searchable claims could be searched without effort justifying an additional fee, the International Searching Authority did not invite payment of any additional fee.

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.

BNSDOCID: <EP___0422230A1_I_>

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.